Az 5G hálózatok ideálisak lesznek az államok közti kiberkaratéhoz

Az Európai Bizottság friss jelentése szerint nem kérdés, hogy szükség van az új generációs infrastruktúrára, de tisztában kell lenni annak kockázataival is.

Az Európai Bizottság szerdai közleményében ismertette azt a jelentést, amelyet az uniós Hálózat- és Információbiztonsági Ügynökséggel (ENISA) közösen állított össze az ötödik generációs (5G) hálózatok kockázatairól. Ezt jelentős lépésnek nevezik annak a márciusi EB-ajánlásnak az implementációjában, amelynek célja a magas szintű kiberbiztonsági standardok megteremtése az új európai hálózati infrastruktúrában. A jelentés kitér a digitalizálódó társadalom és gazdaság gerincének tekintett rendszereket fenyegető veszélyekre, a veszélyt jelentő szereplőkre, a hálózatok legérzékenyebb elemeire, a technológiai vagy más jellegű sérülékenységekre, illetve az 5G hálózatok alkalmazásának stratégiai rizikójára.

A riport külön meghatározza azokat a lényeges biztonsági kihívásokat, amelyek a ma működő rendszerekkel összehasonlítva sokkal jellemzőbbek lehetnek majd az 5G-re. Ezek általában az 5G-vel kapcsolatos innovációkat jelentik, vagyis az olyan szoftvermegoldásokat és szolgáltatásokat, amelyeket eleve az új hálózati technológia tesz lehetővé, illetve a beszállítók szerepét a hálózatok kiépítésében és működtetésében.

Az 5G magasabb fokú szoftveres expozíciója önmagában is nagyobb kitettséget jelent a támadásokra, nem beszélve a potenciális behatolási pontok szaporodásáról. Itt olyan szempontok merülnek fel, mint például a beszállítók esetlegesen hanyag vagy rosszul szabályozott fejlesztési folyamatai, ezen kívül a rosszindulatú szereplőknek is könnyebb dolga van nehezen felfedezhető a hátsó kapuk elhelyezésére az egyes termékekben. A jelentés ehhez kapcsolódóan azt is megjegyzi, hogy az 5G hálózatok architekturális sajátosságai és új feladatai különösen érzékennyé tesznek bitonyos hálózati eszközöket és funkciókat.

Sokféle és alaposan átvilágított beszállítót szeretnének

A kockázatok kezelésében felértékelődik az operátorok és a beszállítók szerepe, nem csak a korábbinál nagyobb felületet nyújtva a támadóknak, de felerősítve a támadások lehetséges hatásait is. Az 5G hálózatokat az EB értékelése szerint leginkább az Európai Unión kívüli államok, illetve az állami szponzorációval dolgozó hekkerek veszik majd célba, ebben a kontextusban pedig nagyon fontos az egyes beszállítók kockázati profiljának meghatározása is, mondjuk abban a tekintetben, hogy működésükbe mennyire esélyes egy másik, nem EU-s kormányzat beavatkozása.

A dokumentum egyébként itt is és más helyeken is kínosan kerüli a Huawei vagy más gyártók név szerinti említését, de a hosszadalmas körülírások mögött nyilván a már sokszor tárgyalt kifogások állnak. Főleg, hogy a jelentés alapvető kockázati tényezőként azonosítja kevés számú nagy beszállítótól való függőséget, ami fenyegethet a szállítási folyamatok szándékos vagy piaci eseményekből eredő megszakításával, de ott van a telekommunikációs szolgáltatóknál tapasztalható szakértelemdeficit kérdése is, ami szintén függőségi helyzethez vezethet egy-egy üzleti partnerrel szemben.

Túl a bizalmas információ vagy a személyes adatok védelmén, az 5G hálózatok esetében is a rendelkezésre állás és az integritás a két legfontosabb

érték, ami uniós és nemzetállami szinten is prioritássá válik a kritikus infokommunikációs alkalmazások megjelenésével. Ez szükségessé teszi a jelenlegi biztonsági és szabályozási keretrendszerek átgondolását az új biztonsági paradigma jegyében, figyelembe véve, hogy ezeket a tagállamoknak is alkalmazniuk kell tudni az IKT szektorban és a hozzá kapcsolódó ökoszisztémában a kockázatok mérséklésére.

A Bizottság ütemezése alapján az illetékes uniós együttműködési csoportnak ez év végéig kellene meghatároznia a fenti rizikók kezeléséhez szükséges, uniós és állami szintű eszközöket. A tagállamoknak jövő októberre értékelniük kellene az EB-vel együtt a szóban forgó eszközök hatékonyságát, és el kell dönteniük, hogy szükség van-e további lépésekre. Maga az Európai Bizottság az Európai Tanács támogatásával március végén adta ki az 5G hálózatok kiberbiztonságát érintő ajánlását, az uniós országok pedig azóta el is juttatták saját megállapításaikat az EB-hez és az ENISA-hoz.

A támadók eközben mi mást tennének, mint támadnak

Ehhez kapcsolódik, hogy a francia kibervédelmi ügynökség (ANSSI) majdnem az Európai Bizottság közleményével egy időben adott ki figyelmeztetést a telekommunikációs szolgáltatók és műszaki vállalatok infrastuktúráját célzó kampányokról, amelyek célja az adatlopás mellett az érintett cégek ügyfeleinek hálózataihoz való hozzáférés. A hétfői közlemény azoknak az információknak az elemzése nyomán született meg, amelyek a különböző szervezetek kiberbiztonsági incidensekre történő reagálásáról szóló beszámolóival jutottak el az ügynökséghez.

Az ANSSI a támadások két hullámát azonosította, amelyek között technikai értelemben még nem talált összefüggést, és sem az áldozatokat, sem a valószínűsíthető forrásokat nem nevezte meg, de a leírásban szereplő malware-ek a kommentárok szerint olyan kódok, amelyek a kínai állami hátterű hekkercsoportokra voltak jellemzők az elmúlt évtizedben. Mindez egy olyan trendbe illeszkedne, amelyben már világszerte célponttá váltak bizonyos felhőszolgáltatók (HPE, IBM, Visma), a francia Airbus és az Expleo, a brit Rolls-Royce, vagy olyan német cégóriások, mint a ThyssenKrupp, a BASF, a Siemens, a Henkel vagy a Bayer.

Forrás: https://bitport.hu/az-5g-halozatok-idealisak-lesznek-az-allamok-kozti-kiberkaratehoz

Válogatta: Fonyó Istvánné